EXHIBIT B

PLR 4-3(a) – Constructions on Which the Parties Agree

Claim Term / Phrase	Agreed Construction
Entity 891.1	Any person or organization.
Generating 861.58	Producing.
Govern, governed, governing 891.1, 683.2	See Control (v.).
Metadata information 861.58	Information that describes one or more attributes of other data, and/or the processes used to create and/or use that data. For example, metadata information may describe the following attributes of other data: its meaning, representation in storage, what it is used for and by whom, context, quality and condition, location, ownership, or its data elements or their attributes (name, size, data type, etc.)
Rendering 193.11, 193.15, 193.19	In the context of 193.11, 15 and 19: Playing content through an audio output (e.g., speakers) or displaying content on a video output (e.g., a screen).
Secure container rule 683.2	A Rule that Governs a Secure Container Governed Item.
Security 721.1, 721.34	See Secure.
Tampering 683.2, 721.1, 721.34, 900.155	Using (e.g., observing or altering) in any unauthorized manner, or interfering with authorized use.
"said mass storage storing tamper resistant software" 900.155	The Tamper Resistant Software is physically stored within, as opposed to being merely Addressed by, the mass storage.
"including using said key to decrypt at least a portion of said first digital file" 193.19	The "at least one use of said digital file" must encompass decrypting at least a Portion of the Digital File using the Key.

Notation:

Each term is followed by a list of the claims in which it appears (e.g., "193.15" means claim 15 from the '193 patent).

'193 patent = U.S. Patent No. 6,253,193
'683 patent = U.S. Patent No. 6,185,683
'721 patent = U.S. Patent No. 6,157,721
'891 patent = U.S. Patent No. 5,982,891
'861 patent = U.S. Patent No. 5,920,861
'912 patent = U.S. Patent No. 5,917,912
'900 patent = U.S. Patent No. 5,892,900

PLR 4-3(b) – InterTrust's Construction of Disputed Terms & Phrases

Claim Term / Phrase	InterTrust Construction
access, accessed, access to, accessing 193.15, 193.19, 912.8, 912.35, 861.58, 683.2, 721.34	To obtain something so it can be used.
addressing 861.58	Referring by specific location or individual name to something without directly storing it.
allowing, allows 912.35, 193.1, 193.11, 193.15, 193.19	Normal English: permitting, permits; letting happen, lets happen.
arrangement 721.34	Normal English: a collection of things that have been arranged. In context, the term can apply to an organization of hardware and/or software and/or data.
aspect 900.155, 912.8, 861.58, 683.2	Feature, element, property or state.
associated with 912.8, 193.1, 193.11, 193.15, 683.2	Having a relationship with.
authentication 193.15	Identifying (e.g., a person, device, organization, document, file, etc.). Includes uniquely identifying or identifying as a member of a group.
authorization information, authorized, not authorized 193.15, 193.19	Authorize: Normal English: permit. Authorization Information: Information (e.g., a key) received if an action is Authorized. Information: nonaccidental signal(s) or character(s) used in a computer or communication system. Information includes programs and also includes data.
budget control; budget 193.1	Budget: Information specifying a limitation on usage. See Authorization Information for the definition of Information. Budget control: The term is explicitly defined in the claim as a Control "including a budget specifying the number of copies which can be made of said digital file."
can be 193.1	Normal English: the specified act is able or authorized to be carried out. In context, this means the number of copies allowed to be made.
capacity 683.2	Normal English: "ability," or "capability."
clearinghouse 193.19	A provider of financial and/or administrative services for a number of Entities; or an entity responsible for the collection, maintenance, and/or distribution of materials, information, licenses, etc.

Claim Term / Phrase	InterTrust Construction
compares, comparison 900.155	Normal English: Compares: examines for the purpose of noting similarities and differences. Comparison: the act of comparing.
component assembly 912.8, 912.35	Components are code and/or data elements that are independently deliverable. A Component Assembly is two or more components associated together. Component Assemblies are utilized to perform operating system and/or applications tasks.
contain, contained, containing 683.2, 912.8, 912.35	Normal English: to have within or to hold. In the context of an element contained within a data structure (e.g., a secure container), the contained element may be either directly within the container or the container may hold a reference indicating where the element may be found.
control (n.) 193.1, 193.11, 193.15, 193.19, 891.1	Information and/or programming Governing operations on or use of Resources (e.g., content) including (a) permitted, required or prevented operations, (b) the nature or extent of such operations or (c) the consequences of such operations.
controlling, control (v.) 861.58, 193.1	Normal English: to exercise authoritative or dominating influence over; direct.
copied file 193.11	A Digital File that has been Copied and is usable.
copy, copied, copying 193.1, 193.11, 193.15, 193.19	Reproduce, reproduced, reproducing. The reproduction must be usable, may incorporate all of the original item or only some of it, and may involve some changes to the item as long as the essential nature of the content remains unchanged.
copy control 193.1	A Control used to determine whether a Digital File may be Copied and the Copied Digital File stored on a second device.
data item 891.1	A unit of digital information.
derive, derives 900.155	Normal English: obtain, receive or arrive at through a process of reasoning or deduction. In the context of computer operations, the "process of reasoning or deduction" constitutes operations carried out by the computer.
descriptive data structure 861.58	Machine-readable description of the layout and/or contents of a rights management data structure (e.g., a Secure Container).
designating 721.1	Normal English: indicating, specifying, pointing out or characterizing.
device class 721.1	A group of devices which share at least one attribute.
digital file 193.1, 193.11, 193.15, 193.19	A named collection of digital information.
digital signature, digitally signing 721.1	Digital signature: A digital value, verifiable with a Key, that can be used to determine the source and/or integrity of a signed item (e.g., a file, program, etc.). Digitally signing is the process of creating a digital signature.

Claim Term / Phrase	InterTrust Construction
entity's control 891.1	Entity's Control: Control belonging to or coming from an Entity. See list of Agreed Constructions for definition of Entity.
environment 912.35, 900.155, 891.1, 683.2, 721.34	Capabilities available to a program running on a computer or other device or to the user of a computer or other device. Depending on the context, the environment may be in a single device (e.g., a personal computer) or may be spread among multiple devices (e.g., a network).
executable programming, executable 912.8, 912.35, 721.34	A computer program that can be run, directly or through interpretation.
execution space, execution space identifier 912.8	Execution space: Resource which can be used for execution of a program or process. Execution space identifier: Information Identifying an Execution Space. See Authorization Information for definition of Information.
governed item 683.2	Governed Item: an item that is Governed. See list of Agreed Constructions for the definition of Governed.
halting 900.155	Normal English: suspending.
host processing environment 900.155	This term is explicitly defined in the claim and therefore needs no additional definition. It consists of those elements listed in the claim. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: a Protected Processing Environment incorporating software-based Security.
identifier, identify, identifying 193.11, 193.15, 912.8, 912.35, 861.58	Identifier: Information used to Identify something or someone (e.g., a password). Identify/identifying: Normal English: To establish/establishing the identity of or to ascertain/ascertaining the origin, nature, or definitive characteristics of; includes identifying as an individual or as a member of a group.
including 193.1 (at 320:63, and 321:3); 193.19 (at 324:15); 912.8 (at 327:36, 39, and 41); 912.35 (330:35 and 39); 861.58 (at 26:53 and 63); and 683.2 (at 63:60).	Normal English: Depending on the context, this means: part of or storing within, as opposed to Addressing.
information previously stored 900.155	Normal English: Information stored at an earlier time. See Authorization Information for the definition of Information.
integrity programming 900.155	This term is fully defined in the claim, which specifies the steps the integrity programming must perform. Integrity programming is programming that performs the recited steps. The term therefore needs no additional definition. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: programming that checks the integrity of a Host Processing Environment.

Claim Term / Phrase	InterTrust Construction
key 193.19	Information used to encrypt, decrypt, sign or verify other information.
load module 912.8, 721.1	An Executable unit of code designed to be loaded into memory and executed, plus associated data.
machine check programming 900.155	Programming that checks a host processing environment and derives information from an Aspect of the Host Processing Environment.
opening secure containers 683.2	Providing Access to the contents of a Secure Container (e.g., by decrypting the contents, if the contents are encrypted).
operating environment 891.1	Environment in which programs function.
organization, organization information, organize 861.58	In the context of organization of a Secure Container, these terms describe contents required or desired (including Information used to categorize these contents); or Information used to specify a particular location for content. See Authorization Information for the definition of Information.
portion 193.1, 193.11, 193.15, 193.19, 912.8, 912.35, 861.58	Normal English: a part of a whole. The presence of a "portion" does not exclude the presence of the whole (e.g., storage of an entire file necessarily includes storage of any portions into which that file may be subdivided).
prevents 721.34	Normal English: keeps from happening.
processing environment 912.35, 900.155, 721:34, 683.2	Processing: manipulating data. Processing Environment: An Environment used for Processing. A Processing Environment may be made up of one device or of more than one device linked together.
protected processing environment 721.34, 683.2	Processing Environment in which processing and/or data is at least in part protected from Tampering. The level of protection can vary, depending on the threat.
protecting 683.2	Normal English: keeping from being damaged, attacked, stolen or injured.
record (n.) 912.8, 912.35	Collection of related items of data treated as a unit.
required 912.8, 861.58	Normal English: a thing that is required is a thing that is obligatory or demanded.
resource processed 891.1	Resource: computer software, computer hardware, data, data structure or information. Resource processed: a Resource subject to being Processed, i.e., computer software, data, data structure or information. See Processing Environment for a definition of Processed.
rule 861.58, 683.2	See Control.

Claim Term / Phrase	InterTrust Construction
secure 193.1, 193.11, 193.15, 912.35, 861.58, 891.1, 683.2, 721.34	One or more mechanisms are employed to prevent, detect or discourage misuse of or interference with information or processes. Such mechanisms may include concealment, Tamper Resistance, Authentication and access control. Concealment means that it is difficult to read information (for example, programs may be encrypted). Tamper Resistance and Authentication are separately defined. Access control means that Access to information or processes is limited on the basis of authorization. Security is not absolute, but is designed to be sufficient for a particular purpose.
secure container 912.35, 861.58, 683.2	Container: Digital File Containing linked and/or embedded items. Secure Container: A Container that is Secure.
secure container governed item 683.2	Information and/or programming Contained in a Secure Container and Governed by an associated Secure Container Rule.
secure database 193.1, 193.11, 193.15	Database: an organized collection of information. Secure Database: Database that is Secure.
secure execution space 721.34	Execution Space that is Secure.
secure memory, memory 193.1, 193.11, 193.15	Memory: A medium in which data (including executable instructions) may be stored and from which it may be retrieved. "Memory" includes "virtual memory." Secure Memory: Memory in which Information is handled in a Secure manner. See Authorization Information for the definition of Information.
secure operating environment, said operating environment 891.1	An Operating Environment that is Secure.
securely applying 891.1	Requiring that one or more Controls be complied with before content may be used. The operation of requiring that the Control(s) be complied with must be carried out in a Secure manner.
securely assembling 912.8, 912.35	Associating two or more Components together to form a Component Assembly, in a Secure manner. See Component Assembly for the definition of Component.
securely processing 891.1	Processing occurring in a Secure manner. See Processing Environment for the definition of Processing.
securely receiving 891.1	Receiving has its normal English meaning: acquiring or getting. Securely Receiving means receipt occurring in a Secure manner.
security level, level of security 721.1; 721.34, 912.8	Information that can be used to determine how Secure something is (e.g., a device, Tamper Resistant Barrier or Execution Space).
tamper resistance 721.1, 721.34, 900.155	Making Tampering more difficult and/or allowing detection of Tampering.
tamper resistant barrier 721.34	Hardware and/or software that provides Tamper Resistance.

Claim Term / Phrase	InterTrust Construction
tamper resistant software 900.155	Software designed to make it more difficult to Tamper with the software and/or allow detection of tampering.
use 912.8, 912.35, 861.58, 193.19, 891.1, 683.2, 721.1	Normal English: to put into service or apply for a purpose, to employ.
user controls 683.2	Hardware feature of an apparatus allowing a user to operate the apparatus (e.g., a keyboard).
validity 912.8	A property of something (e.g., a Record) indicating that it is appropriate for use.
virtual distribution environment 900.155	This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: secure, distributed electronic transaction management and rights protection system for controlling the distribution and/or other usage of electronically provided and/or stored information.
'193:1	The claim contains no requirement of a VDE.
receiving a digital file including music	See Receiving a digital file (193.11). This phrase is interpreted the same, except that the file includes music.
a budget specifying the number of copies which can be made of said digital file	Normal English, incorporating the separately defined terms: a Budget stating the number of Copies that Can Be made of the Digital File referred to earlier in the claim.
controlling the copies made of said digital file	The nature of this operation is further defined in later claim elements. In context, the Copy Control determines the conditions under which a Digital File may be Copied and the Copied File stored on a second device.
determining whether said digital file may be copied and stored on a second device based on at least said copy control	Normal English, incorporating the separately defined terms: Using the Copy Control in deciding whether the Digital File referred to earlier in the claim may be Copied and the Copied Digital File stored on a second device.
if said copy control allows at least a portion of said digital file to be copied and stored on a second device	Normal English: a "yes" result is received in the step Determining whether said digital file may be copied and stored on a second device based on at least said copy control (193.1).
copying at least a portion of said digital file	Normal English, incorporating the separately defined terms: Copying at least a Portion of the Digital File referred to earlier in the claim.
transferring at least a portion of said digital file to a second device	Normal English, incorporating the separately defined terms: at least a Portion of the Copied Digital File is sent to a second device.
storing said digital file	Normal English: that which was transferred in the transferring step is stored.
'193:11	The claim contains no requirement of a VDE.
receiving a digital file	Normal English, incorporating the separately defined term: a Digital File is obtained. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term:

Claim Term / Phrase	InterTrust Construction
	Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.
determining whether said digital file may be copied and stored on a second device based on said first control	Normal English, incorporating the separately defined terms: Using the Control to decide whether the Digital File may be Copied and the Copied Digital File stored on the second device.
identifying said second device	Normal English, incorporating the separately defined term: the second device is Identified.
whether said first control allows transfer of said copied file to said second device	Normal English, incorporating the separately defined terms: Using the first Control to decide if the Copied Digital File may be sent to the second device.
said determination based at least in part on the features present at the device	Normal English: the decision referred to earlier in the claim is based at least in part on characteristics of the second device.
if said first control allows at least a portion of said digital file to be copied and stored on a second device	See "If said copy control allows at least a portion of said digital file to be copied and stored on a second device" (193.1). The definitions are the same.
copying at least a portion of said digital file	See "Copying at least a portion of said digital file" (193.1). The definitions are the same.
transferring at least a portion of said digital file to a second device	See "Transferring at least a portion of said digital file to a second device" (193.1). The definitions are the same.
storing said digital file	See "Storing said digital file" (193.1). The definitions are the same.
'193:15	The claim contains no requirement of a VDE.
receiving a digital file	See "Receiving a digital file" (193.11). The definitions are the same.
an authentication step comprising:	Normal English, incorporating the separately defined term: a step involving Authentication.
accessing at least one identifier associated with a first device or with a user of said first device	Normal English, incorporating the separately defined terms: Accessing an Identifier Associated With a device or a user of the device.
determining whether said identifier is associated with a device and/or user authorized to store said digital file	Normal English, incorporating the separately defined terms: deciding whether the Identifier is Associated With a device or user with authority to store the Digital File.
storing said digital file in a first secure memory of said first device, but only if said device and/or user is so authorized, but not proceeding with said storing if said device and/or user is not authorized	Normal English, incorporating the separately defined terms: this step proceeds or does not proceed based on the preceding determining step. If this step proceeds, the Digital File is stored in a Secure Memory of the first device.
storing information associated with said digital file in a secure database stored on said first device, said information including	Normal English, incorporating the separately defined terms: storing a Control Associated With the Digital File in a Secure Database stored at the first device.

Claim Term / Phrase	InterTrust Construction
at least one control	
determining whether said digital file may be copied and stored on a second device based on said at least one control	See "Determining whether said digital file may be copied and stored on a second device based on at least said copy control" (193.1). The definitions are the same.
if said at least one control allows at least a portion of said digital file to be copied and stored on a second device,	See "If said first control allows at least a portion of said digital file to be copied and stored on a second device" (193.11). The definitions are the same.
copying at least a portion of said digital file	See "Copying at least a portion of said digital file" (193.1). The definitions are the same.
transferring at least a portion of said digital file to a second device	See "Transferring at least a portion of said digital file to a second device" (193.1) The definitions are the same.
storing said digital file	See "Storing said digital file" (193.1) The definitions are the same.
'193:19	The claim contains no requirement of a VDE.
receiving a digital file at a first device	See "Receiving a digital file" (193.11). The definitions are the same.
establishing communication between said first device and a clearinghouse located at a location remote from said first device	Normal English, incorporating the separately defined term: sending information from the first device to the Clearinghouse and/or the first device receiving information from the Clearinghouse. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term: Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.
using said authorization information to gain access to or make at least one use of said first digital file	Normal English, incorporating the separately defined terms: the Authorization Information is used in a process of Accessing or Using the Digital File.
receiving a first control from said clearinghouse at said first device	Normal English, incorporating the separately defined terms: the first device acquires or gets a Control from the Clearinghouse. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term: Claim elements specifying the act of receiving a file, or the act of establishing communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc.
storing said first digital file in a memory of said first device	Normal English, incorporating the separately defined terms: the Digital File is stored at the first device.

Claim Term / Phrase	InterTrust Construction
using said first control to determine whether said first digital file may be copied and stored on a second device	See "Determining whether said digital file may be copied and stored on a second device based on at least said copy control" (193.1). The definitions are the same.
if said first control allows at least a portion of said first digital file to be copied and stored on a second device	See "If said first control allows at least a portion of said digital file to be copied and stored on a second device" (193.11). The definitions are the same.
copying at least a portion of said first digital file	See "Copying at least a portion of said digital file" (193.1). The definitions are the same.
transferring at least a portion of said first digital file to a second device including a memory and an audio and/or video output	See "Transferring at least a portion of said digital file to a second device" (193.1). The definitions are the same, except that the second device has an audio or video output or both (e.g., a speaker, a screen, etc.).
storing said first digital file portion	Normal English, incorporating the separately defined terms: the Digital File Portion is stored.
'683:2	The claim contains no requirement of a VDE.
the first secure container having been received from a second apparatus	Normal English, incorporating the separately defined term: the Secure Container was acquired from a second apparatus. The second apparatus is different from the first apparatus.
an aspect of access to or use of	Normal English, incorporating the separately defined terms: Aspect and Access to or Use of. Those terms fully define the phrase, so that no other definition is possible.
the first secure container rule having been received from a third apparatus different from said second apparatus	Normal English, incorporating the separately defined terms: this term requires that the first Secure Container Rule was acquired from a third apparatus. The third apparatus is different from the second apparatus or the first apparatus.
hardware or software used for receiving and opening secure containers	Normal English, incorporating the separately defined terms: computer hardware or programming that acquires Secure Containers and Opens the Secure Containers (see Opening Secure Containers). This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies structures corresponding to this term: Structures corresponding to this element include Processor(s) 4126 and/or software running on Processors 4126 (including Protected Processing Environment 650) and Communications Device 666.
said secure containers each including the capacity to contain a governed item, a secure container rule being associated with each of said secure containers	Each Secure Container referred to in the phrase "hardware or software used for receiving and opening secure containers" must have the capacity to Contain a Governed Item, and must have Associated With it a Secure Container Rule.
protected processing environment at least in part protecting information contained in said protected processing environment from tampering by a user of said first apparatus	Normal English, incorporating the separately defined terms: a Protected Processing Environment contains Information. The Protected Processing Environment protects the contained Information from Tampering by a user. The protection may be partial rather than complete. See Authorization Information for the definition of Information.

Claim Term / Phrase	InterTrust Construction
hardware or software used for applying said first secure container rule and a second secure container rule in combination to at least in part govern at least one aspect of access to or use of a governed item contained in a secure container	Normal English, incorporating the separately defined terms: computer hardware or programming that uses the first Secure Container Rule and a second Secure Container Rule. These rules are Applied in Combination to Govern a Governed Item contained in a Secure Container. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies structures corresponding to this term: Structures corresponding to this element include Processor(s) 4126 and/or software running on Processors 4126 (including Protected Processing Environment 650).
hardware or software used for transmission of secure containers to other apparatuses or for the receipt of secure containers from other apparatuses.	Normal English, incorporating the separately defined terms: computer hardware or programming that sends Secure Containers to other apparatuses (e.g., other computers) or acquires Secure Containers from other apparatuses. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies structures corresponding to this term: Structures corresponding to this element include Processor(s) 4126 and/or software running on Processors 4126 (including Protected Processing Environment 650) and Communications Device 666.
'721:1	The claim contains no requirement of a VDE.
digitally signing a first load module with a first digital signature designating the first load module for use by a first device class	Normal English, incorporating the separately defined terms: generating a Digital Signature for the first Load Module, the Digital Signature Designating that the first Load Module is for use by a first Device Class.
digitally signing a second load module with a second digital signature different from the first digital signature, the second digital signature designating the second load module for use by a second device class having at least one of tamper resistance and security level different from the at least one of tamper resistance and security level of the first device class	Normal English, incorporating the separately defined terms: generating a Digital Signature for the second Load Module, the Digital Signature Designating that the second Load Module is for use by a second Device Class. This element further requires that the second Device Class have a different Tamper Resistance or Security Level than the first Device Class.
distributing the first load module for use by at least one device in the first device class	Normal English, incorporating the separately defined terms: distributing the first Load Module so that it can be used by a device in the first Device Class.
distributing the second load module for use by at least one device in the second device class	Normal English, incorporating the separately defined terms: distributing the second Load Module so that it can be used by a device in the second Device Class.
'721:34	The claim contains no requirement of a VDE.
arrangement within the first tamper resistant barrier	Normal English, incorporating the separately defined terms: an Arrangement protected by the first Tamper Resistant Barrier, the Arrangement operating as described in the claim.

Claim Term / Phrase	InterTrust Construction
prevents the first secure execution space from executing the same executable accessed by a second secure execution space having a second tamper resistant barrier with a second security level different from the first security level	Normal English, incorporating the separately defined terms: stops the first Secure Execution Space from executing (e.g. running a program) an Executable accessed by a second Secure Execution space. The first and second Secure Execution Spaces have Tamper Resistant Barriers that have different Security Levels.
'861:58	The claim contains no requirement of a VDE.
creating a first secure container	This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: Normal English, incorporating the separately defined terms: producing a Secure Container.
including or addressing . . . organization information . . . desired organization of a content section. . . and metadata information at least in part specifying at least one step required or desired in creation of said first secure container	This is not a claim term, but is instead a series of fragments. Interpretation of this phrase is therefore impossible, since the phrase does not appear in the claim. Without waiving its position that these claim fragments should not be interpreted, InterTrust would be willing to agree to the following: 1. The same single Descriptive Data Structure must either Contain within its confines or Address both Organization Information and Metadata information.
at least in part determine specific information required to be included in said first secure container contents	Normal English, incorporating the separately defined terms: at least partially Identify specific Information that must be included in the first Secure Container. See Authorization Information for the definition of Information.
rule designed to control at least one aspect of access to or use of at least a portion of said first secure container contents	Normal English, incorporating the separately defined terms: a Rule that Governs at least some of the contents of the Secure Container.
'891:1	The claim contains no requirement of a VDE.
resource processed in a secure operating environment at a first appliance	This term is contained in the preamble of the claim and should not be defined, other than as requiring the individual claim elements. Without waiving its position that no separate definition is required, if required to propose such a definition, InterTrust proposes the following: Normal English, incorporating the separately defined terms: a Resource Processed in a Secure Operating Environment, the Secure Operating Environment being present at an appliance (e.g., a computer).
securely receiving a first entity's control at said first appliance	Normal English, incorporating the separately defined terms: an Entity's Control is Securely Received at the first appliance. This phrase has been designated by Microsoft for interpretation under § 112(6). InterTrust objects to such designation. Without waiver of such objection, as is required by the Local Rules, InterTrust hereby identifies acts corresponding to this term: Claim elements specifying the act of receiving a file, or the act of establishing

Claim Term / Phrase	InterTrust Construction
	communications, map onto a large number of structures and acts disclosed in the specification, many of which constitute alternate embodiments. These include obtaining a file or communicating through telecommunications links, satellite transmissions, physical exchange of media, network transmissions, etc. Claim elements specifying the act of "securely receiving" map onto embodiments of "receiving" (see above) in which the received element (e.g., a control) is received in a manner providing security. The specification describes a number of security-related mechanisms for use in communications, including encryption, authentication and tamper-resistance. Such mechanisms constitute alternate embodiments.
securely receiving a second entity's control at said first appliance	See Securely receiving a first entity's control at said first appliance. The definitions are the same, except that the second entity and the first entity are different.
securely processing a data item at said first appliance, using at least one resource	Normal English, incorporating the separately defined terms: a Resource is used in Securely Processing a Data Item, the processing occurring at the first appliance.
securely applying, at said first appliance through use of said at least one resource said first entity's control and said second entity's control to govern use of said data item	Normal English, incorporating the separately defined terms: the first Entity's Control and the second Entity's Control are Securely Applied to Govern Use of the Data Item, the act of Securely Applying involving use of the Resource.
'900:155	See definition of Virtual Distribution Environment, above.
first host processing environment comprising	A Host Processing Environment including (but not limited to), the listed elements.
designed to be loaded into said main memory and executed by said central processing unit	Normal English, incorporating the separately defined term: software designed to be loaded into the Memory of a computer and executed by the computer's processor.
said tamper resistant software comprising: . . . one or more storage locations storing said information	This is not a claim term, but is instead two sentence fragments. Interpretation of this phrase is therefore impossible, since the phrase does not appear in the claim.
derives information from one or more aspects of said host processing environment,	Normal English, incorporating the separately defined terms: Derives (including creates) Information based on at least one Aspect of the previously referred to Host Processing Environment. See Authorization Information for the definition of Information.
one or more storage locations storing said information	Normal English, incorporating the separately defined terms: Information relating to one or more Aspects of the Host Processing Environment is stored in one or more locations. See Authorization Information for the definition of Information.
information previously stored in said one or more storage locations	See Information Previously Stored. The definitions are the same.
generates an indication based on the result of said comparison	Producing an indication based on the result of the "compares" step. The "indication" need not be displayed to a user.
programming which takes one or more actions based on the state of said indication	Normal English: software that takes an action if the indication has one state, but does not take that action if the indication does not have that state.
at least temporarily halting further processing	Normal English, incorporating the separately defined terms: Halting Processing, the Halt being temporary or permanent. See Securely Processing for the definition of Processing.

Claim Term / Phrase	InterTrust Construction
	Processing.
'912:8	The claim contains no requirement of a VDE.
identifying at least one aspect of an execution space required for use and/or execution of the load module	Identifying at least one aspect of an execution space: Normal English, incorporating the separately defined terms: Identifying an Aspect (e.g. Security Level) of an Execution Space Required for use and/or execution of the load module: Normal English, incorporating the separately defined terms: the Identified Aspect is needed in order for the Load Module to execute or otherwise be used.
said execution space identifier provides the capability for distinguishing between execution spaces providing a higher level of security and execution spaces providing a lower level of security	Normal English, incorporating the separately defined terms: the Execution Space Identifier makes it possible to distinguish higher Security Level Execution Spaces from lower Security level Execution Spaces.
checking said record for validity prior to performing said executing step	Normal English, incorporating the separately defined terms: determining whether the Record has Validity, the determination occurring before the execution step.
'912:35	The claim contains no requirement of a VDE.
received in a secure container	Normal English, incorporating the separately defined terms: the Record is Contained in a Secure Container when acquired.
said component assembly allowing access to or use of specified information	Normal English, incorporating the separately defined terms: the Component Assembly allows Access to specified Information. See Authorization Information for the definition of Information.
said first component assembly specified by said first record	This term is a label referring back to the first component assembly identified earlier in the claim. It has no other meaning.